An Optimized Node Selection Routing Protocol for Vehicular Ad-hoc Networks – A Hybrid Model

Thangakumar Jeyaprakash, and Rajeswari Mukesh

Abstract— **Vehicular Ad-hoc networks (VANETs) are a subset of Mobile Ad-hoc Networks made by vehicles communicating among themselves on roadways. The Routing protocols implemented for MANETs such as Ad-hoc on Demand Distance Vector Routing Protocol (AODV), Dynamic Source Routing (DSR), and Destination Sequence Distance Vector Routing Protocol (DSDV) are not suitable for VANET due to high Mobility. Trusted routing in VANET is a challenging task due to highly dynamic network topology and openness of wireless architecture. To avoid a frequent communication link failure, to reduce the communication overhead and to provide a trusted routing among the vehicular nodes for achieving high packet transmission, we implemented an Optimized Node Selection Routing protocol (ONSRP) of VANET based on Trust. In our proposed work, we implemented an enhanced routing protocol which prevents the network from communication link failure frequently. The testing results stated that the ONSRP routing have a high performance measures than the above mentioned existing routing protocols.**

Keywords- Vehicular Ad-hoc networks (VANET), Routing, Trust.

I. Introduction

Vehicle to Vehicle to Communication (V2V) for passengers safety is the dynamic wireless transmission of data between neighbor vehicles that offers the services for important safety improvements. The aim for V2V is that eventually, each vehicle on the highways will be able to communicate with each other through Dedicated Short Range Communication (DSRC) for exchanging the messages dynamically. This V2V communications will provide the active safety measurements that can assist and alert drivers in preventing 76 percent of the crashes on the roadway, thereby reducing fatalities, injuries and major damages that occur each year in India. This is achieved by an efficient routing protocol without communication overhead due to frequent communication link failure. The enhanced routing in VANETs needs to be considering with the various distinct characteristics of MANETs.

Martin Mauve and Jörg Widmer [1] presented an overview of Ad-hoc routing protocols based on the geographical position of the packet's destination. They compared location services protocols such as DREAM (Distance Routing effect Algorithm for mobility), Grid Location services (GIS) etc. "The Security and Privacy of Smart Vehicles" [2] discusses the important evolution for the automotive industry is the one toward context awareness, meaning that a vehicle is aware of its pre-emptively (including the presence and location of other vehicles. Patroklos g. argyroudis et al [3] formulated the threat model for the Ad-hoc networks and mentioned specific attacks that can target the operation of Routing protocol. The several specific attacks discussed in this paper are location disclosure, black hole attack, replay, warmhole attack, Denial of service, routing table poisoning etc. He also compared the set of Secure Ad-hoc routing protocol of MANET and each protocol has a different set of operational requirements and provides protection against different attacks by utilizing particular approaches. Maxim Raya and JeanPierre Hubaux [4] provides a detailed threat analysis such as Bogus information, Cheating with positioning information, ID disclosure of other vehicles, Denial of Service etc. and describes an appropriate security architecture.

Charles Harsch et al [6] proposed a defence mechanism, relying both on cryptographic primitives and plausibility checks mitigating false position injection. They integrated the mechanisms to protect the position-based routing functionality and services (beaconing, multi-hop forwarding, and geo-location discovery), and enhance the network robustness Feilong Tang et al [5] presents a secure routing protocol SecMLR(Secure Maximum Network Lifetime Routing), which can resist most of attacks against routing in WMSNs and work in energy-efficient way. Mohammad Jalali et al [7] proposed a fuzzy reputation system to discipline selfish and encourage packet forwarding. The solution proposed to find the selfish node to be eliminated from the network to increase the network performance.

Khaleel Mershad, Hassan Artail, and Mario Gerla [10] exploited the infrastructure of roadside units (RSUs) to efficiently and reliably route packets in VANETs. The authors evaluated the performance of the system using the ns2 simulation platform and compare the scheme to existing solutions such as TrafRoute protocol and A static-node assisted adaptive routing protocol in vehicular networks Preetida Vinayakray - Jani [9] presented the pre-emptive analysis of MANET and VANET. This paper describes the AODV, DSR, DSDV protocols, associated algorithms and the strength and weakness of these routing protocols. Mushtak Y. Gadkari et al [8] made an attempt for identifying major issues and challenges associated with different VANET protocols, security and simulation tools. Mahmoud Hashem Eiza and Qiang Niused

Manuscript received received February 12, 2015; revised June 12, 2015.

Authors are with the Department of CSE Hindustan Institute of Technology and Science Chennai, India. (E-mails: thang.kumar@gmail.com, rajeswarim@hindustanuniv.ac.in).

[13] provide the evolving graph theory to model the VANET communication graph on a highway. The proposed model captures the evolving characteristics of the vehicular network topology and determines the reliable routes pre-emptively.

Albert Wasef and Xuemin (Sherman) Shen [11] proposed an Expedite Message Authentication Protocol (EMAP) for VANETs, which replaces the time-consuming Certificate Revocation lists checking process by an efficient revocation checking process. Zhengming Li [12] suggest a VANET-based Ambient Ad-Dissemination scheme (VAAD) to support secure ad disseminations with pragmatic cost and effect control. ChiragBhalodia et al [14] mentioned when route break will generate at that time intermediate node send route error packet to source and source has another route in its routing table. This secondary route will work as an active route in data transfer. Mohammad Al-Rabayah et al [15] proposed a new hybrid routing protocol for vanet which combines the features of location based [16] and topology based routing protocol. The route discovery starts with the geographic Routing and again route discovery has been initiated, if the location routing degraded. This will increase the delay in communication among the network.

In upcoming chapters we discussed elaborately about our proposed work and the comparisons over the existing scheme. Section II describes the existing routing protocols such as Modified Ad-hoc on-demand Distance Vector Routing Protocol and Greedy Perimeter Coordinator Routing Protocol. The limitations of existing routing protocols are discussed briefly in section II. In section III A, the proposed work is discussed and we have mentioned the notations of all parameters in Table I. This section focuses more about the proposed implementation and shows the performance over the existing routing protocols. In Section IV, we have implemented the proposed routing protocol using Network Simulator 2 and compared with the existing routing protocols with respect to the performance measures such as packet delivery ratio, throughput and end-end delay.

II. Existing Work

A. Modified AODV Routing Protocol

ChiragBhalodia et al [14] stated when route break occurs, at the same time, the intermediate node will send route error packet to source and source has another route in its routing table. The node broadcasts a route request (RREQ) packet to all its neighbours to find the destination node. The RREQ packet includes source address, source sequence number, broadcast ID, destination address, destination sequence number and hop count. If a neighbor node knows the route to reach the destination node, it replies with the route reply (RRPLY) packet to the source node. The RRPLY contains source address, source sequence number, broadcast ID, destination address, destination sequence number and hop count. The source sequence number specifies the freshness of the information about the reverse route to the source. The destination sequence number specifies the freshness of the route to reach the destination from the source. Otherwise, the neighbor node will forwarded the RREQ until an active route is found to reach the destination. It causes larger delays due to frequent route failure may require a new route discovery. This may decreases the data transmission rate and increases the network overhead.

B. Greedy Perimeter Coordinator Routing

Karp et al [17] proposed GPCR (Greedy Perimeter coordinatorRouting) which uses the closest location of node for the data communication on the basis of distance. The packets are transmitted on a greedy basis by selecting the node closest to the destination. This process repeats until the destination is reached. In some cases the best path may be determined [18]. In such cases, it resumes the greedy process by selecting the best path to reach the destination.

III. Proposed Work

A. Optimized Node Selection Routing Protocol

To avoid the link failure, we have proposed a new enhanced trusted routing protocol algorithm for high Mobility (ONSRP) framework; each node maintains a Flag Trust database routing table that stores the signal strength based on distance, direction and velocity of the nodes and trust information of neighbor nodes. It can therefore be classified as Optimized Node Selection approach. An entry in the routing table includes a source node, destination node, Hop count, Next hop and the Trust value to the node, as well as a time value that indicates when this information was generated. Of course, the accuracy of such an entry depends on the received signal strength. Each node regularly sends the HELLO packets [18] to update the Trust information maintained by the other nodes.

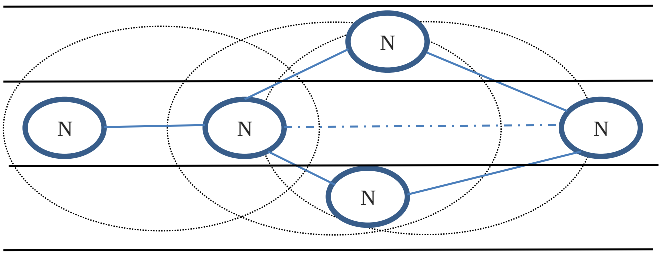


Figure 1. N1, N2, N3, N4, N5 – Nodes in the coverage area of VANET

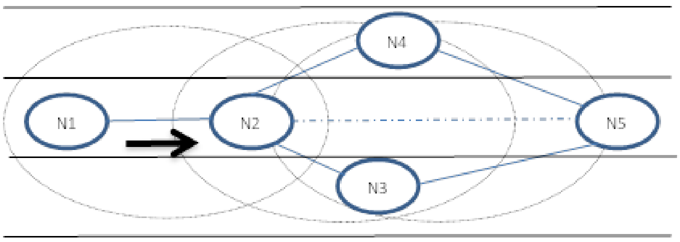


Figure 2. N1 broadcast a route request to send the packet to N5

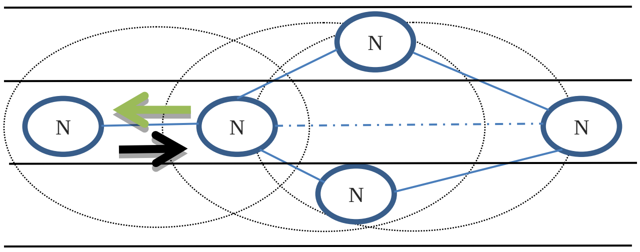


Figure 3. N1 broadcast a route request to send the packet to N5. N2 send a Route Reply to N1 even though the signal is weak

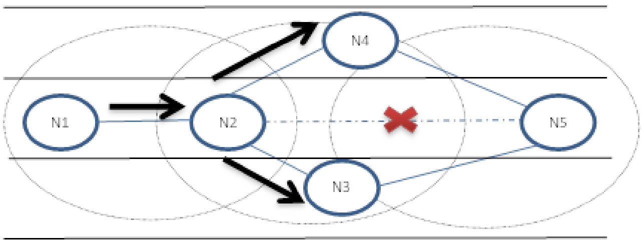
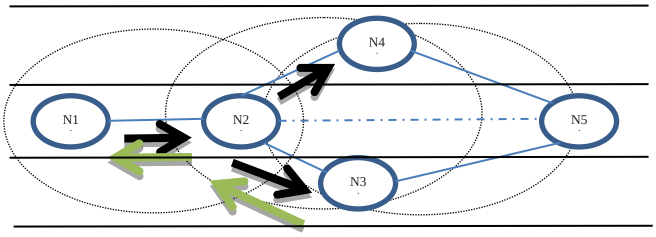


Figure 4. N1 broadcast a route request to send the packet to N5. N2 broadcast the Route request to N3 & N4

Src	Desc	Seq	HOP	FlagT
1	5	134	2	1



Src	Desc	Seq	HOP	FlagT
1	5	136	2	0

Figure 5. N1 broadcast a route request to send the packet to N5. N2 broadcast the Route request to N3 & N4

Fig 1, 2, 3, 4 & 5 shows the Optimized Node selection Routing Protocol Approach. The Flag Trust value changes the Routing table to select the optimized node based on the distance between nodes, direction of the node, velocity of the node and the Trust value.

Let D is the Distance, A is the Direction and V is the Velocity where at Time T1,

$$\text{Distance (Do)} = \text{Minimum (D1||D2||D3…..Dn)} \tag{1}$$

$$\text{Direction in degrees (Ao)} = \text{D (RWP (i, j)) \& Min (D1||D2||D3…Dn) (i, j))} \tag{2}$$

$$\text{Velocity (Vo)} = \text{V (Dn) || V (N1||N2||N3…Nn)} \tag{3}$$

TABLE I
NOTATION

Symbol	Definition
d	Distance in metre per second
do	Optimized distance of the neighbor node of the destination
A	Direction in degrees
Ao	Optimized Direction of the neighbor node of the destination
V	Velocity in speed
Vo	Optimized Velocity of the neighbor node of the destination
Dn	Destination node
RREQ	Route Request from the source node to the destination
RREP	Route Reply
t	Time
RSSI	Received Signal Strength Index
Pt	Transmitted Power
Ct	Tranceiver Constant
Pl	Packet Loss
FlagT	FlagTrust
FlagTcount	FlagTrustCount
PDR	Packet Delivery Ratio
DPr	Packet received at the destination
DPg	Packet Generated at the source
Br	Received bits at the destination

In Table I, we have mentioned the notation of parameters of ONSRP. After the FlagTrust value has been calculated, it will be compared with the threshold value to update the value of FlagTrust in the routing table. Table II shows the FlagTrust value has been updated as 0 & 1.

TABLE II
FLAG TRUST MATRICES

	NI	N2	N3	N4	N5
N1	0	1	0	0	0
N2	1	0	1	1	0
N3	1	0	0	0	1
N4	0	1	0	0	1
N5	0	0	1	1	0

B. FlagTrustAlgorithm

```
Start
for li = (1 to m)
for  nj=(1 to n)
 li – No. of lanes present
 nj– No. of nodes  present in each lanes
{
```

```
(
FlagTrust = $\Sigma i = 1$ to n Do .Ao .Vo .Maximum Trust
Count.
}
for(i=1;i<=m;i++)
{
if FlagTrust = Threshold
Update N==1
Else
0}
Stop
}}
```

IV. Results & Comparisons

We have evaluated the simulation to prove the performance of Optimized node selection routing protocol in three phases using NS2. The proposed protocol has been compared with Modified Ad-hoc on demand distance vector routing protocol and Greedy Perimeter Coordinator Routing Protocol.

A. *Packet Delivery Ratio*

Packet delivery ratio [18] is defined as the ratio of received packet by the destinations to the packet generated from the source. Mathematically, it can be defined as:

$$PDR = DPr / DPg \qquad (4)$$

DPr = sum of packets received by the each destination

DPg = sum of packets generated by the each source

B. *Throughput*

Throughput [18] is defined as the number of bits delivered successfully per second to the destination. Mathematically, it can be defined as:

$$Throughput = Br/1000 \qquad (5)$$

Where

Br = The number of bits received successfully by all Destinations.

C. *End-End Delay*

End to End delay [18] refers both loss time and receive time. Delay refers as how long it takes to reach the destination. Mathematically, it can be defined as:

$$\text{Average end-to-end delay} = S/Br \qquad (6)$$

S = sum of time spent to deliver packets for each destination

Br = number of packets received by the all destination nodes

Practically, we can confirm that the ONSRP is optimal by comparing to the Modified Ad-hoc on demand distance vector Routing protocol and Greedy Perimeter coordinator Routing Protocol with the parameters communication overhead, Throughput and packet delivery ratio. Fig 6, 7, & 8, shows the performance of ONSRP and existing routing protocols. The graph shows a raise in the transmission of packets of ONSRP compared to MAODV and GPCR. Table III shows the simulation parameters of ONSRP.

TABLE III
SIMULATION PARAMETERS

Parameter	Values
Simulation time	1500 seconds
Simulation area	1000 m x 1000 m
Data pay load	512 bytes/packet
Bandwidth	2 Mbps
Routing protocols	MAODV,ONSRP, GPCR
Packet rate	8 Packets/sec
Node pause time	60
Channel Type	Wireless Channel
Antenna type	Omni Directional

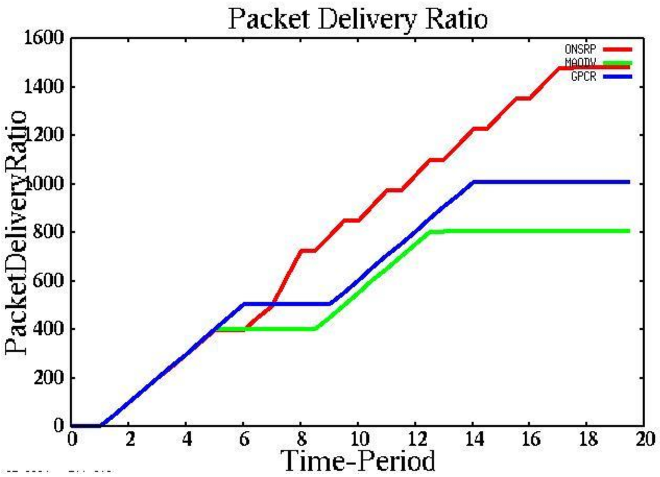


Figure 6. Packet Delivery Ratio plot

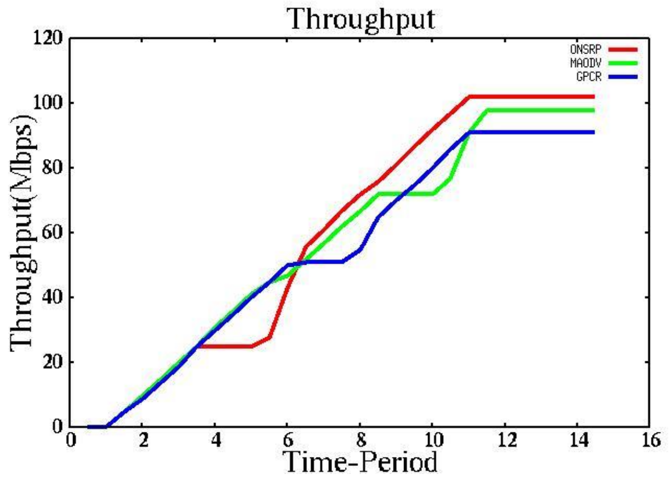


Figure 7. Throughput plot

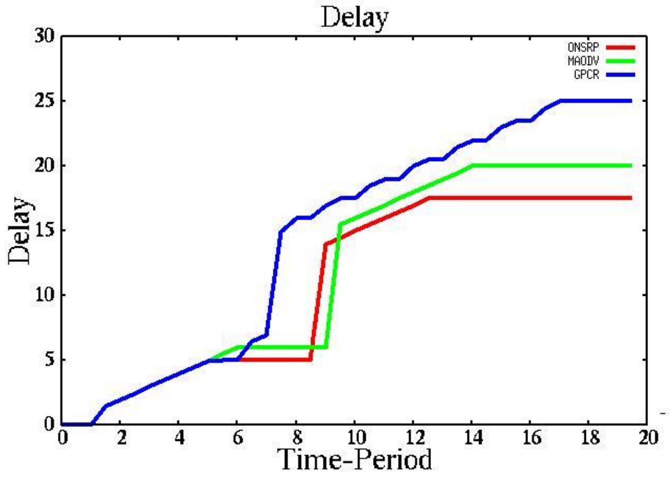


Figure 8. End-End Delay plot

Fig. 6 shows the performance of routing protocols with respect to Packet Delivery Ratio. Fig 7. shows the results of throughput plot. Fig. 8 shows the performance criteria of end-end delay of the existing and proposed routing protocols. We improved the performance of each parameters compared to the existing routing protocols such as MAODV and GPCR with respect to achieving high packet delivery ratio and reducing communication overhead of the Vehicular Ad-hoc Network. The performance metrics such as Delay, Throughput and Packet Delivery ratio for the node density 25, 50 and100 has been implemented in the presence of link failures using Network Simulator. The rate of packet transmission is 8 per seconds.

V. Conclusions & Future Work

We implemented an Optimized node selection routing protocol of VANET with the features of extended light weight routing tables and routing messages with trust information which can be updated directly through optimized node selection Routing protocol Algorithm. When performing trusted routing discovery, communication overhead can be reduced and the packet delivery ratio can be increased by avoiding frequent route discovery process. The results shows the performance of ONSRP eventually exceeds the performance of Modified Ad-hoc On demand distance vector Routing protocol and Greedy Perimeter coordinator Routing Protocol with the aspects of the packet delivery ratio, throughput and End-End Delay. This performance has been proved, but can perhaps be shown to be valid for other existing shortest-path protocols. The scope of the work can move towards the comparison of ONSRP against other proposed routing protocols in an attempt to further support this performance analysis.

References

[1] Martin Mauve and Jörg Widmer, "A Survey on Position-Based Routing in Mobile Ad-hoc Networks", IEEE Network, pp 30-40, December 2001

[2] "The Security and Privacy of Smart Vehicles", Published by The IEEE Computer Society, pp 49 -56, 2004

[3] Patroklos g. Argyroudis et al, "Secure Routing for Mobile Ad-hoc Networks", IEEE communication Surveys, Third Quarter, Volume 7, No 3, pp 2-20, 2005

[4] Maxim Raya and JeanPierre Hubaux, "The Security of Vehicular Ad-Hoc Networks", SASN’05, ACM, Virginia, USA, 2005

[5] Feilong Tang, Minyi, Minglu Li, Cho-Li Wang and Mianxiong Dong, "Secure Routing for Wireless Mesh Sensor Networks in Pervasive Environments", International Journal Of Intelligent Control And Systems Vol. 12, NO. 4, December 2007, 293-306

[6] Charles Harsch "Secure Position-Based Routing for vanet" , IEEE Computer Society, pp 26- 31, 2007

[7] Mohammad Jalali et al, "A Fuzzy Reputation System in Vehicular Ad-hoc Networks", Procedia Computer Science 5 (2011) 951–956

[8] Mushtak Y. Gadkari et al, "vanet: Routing Protocols, Security Issues and Simulation Tools", IOSR Journal of Computer Engineering (IOSRJCE) ISSN: 2278-0661 Volume 3, Issue 3 (July-Aug. 2012), PP 28-38

[9] Preetida Vinayakray Jani, "Routing Protocols For Mobile And Vehicular Ad-Hoc Networks: A Comparative Analysis", Acta Technica Corviniensis, September 2012.

[10] Khaleel Mershad, Hassan Artail, and Mario Gerla, "We Can Deliver Messages to Far Vehicles" ,IEEE Transactions On Intelligent Transportation Systems, Vol. 13, No. 3, September 2012

[11] Albert Wasef and Xuemin (Sherman) Shen, "Emap: Expedite Message Authentication Protocol for Vehicular Ad-Hoc Networks" ,IEEE Transactions On Mobile Computing, Vol. 12, No. 1, January 2013,pp 78 – 90

[12] Zhengming Li, Congyi Liu, and Chunxiao Chigan, "On Secure VANET-Based Ad Dissemination with Pragmatic Cost and Effect Control", IEEE Transactions on Intelligent Transportation Systems, Vol. 14, NO. 1, March 2013, pp 124-136

[13] Mahmoud Hashem Eiza and Qiang Ni, "An Evolving Graph-Based Reliable Routing Scheme for VANETs", IEEE

Transactions On Vehicular Technology, Vol. 62, No. 4, May 2013

[14] ChiragBhalodia et al, "Modified Route Maintenance in AODV Routing Protocol" ,International Journal of Advance Engineering and Research Development (IJAERD) Volume 1,Issue 5,May 2014, e-ISSN: 2348 - 4470,pp 1 - 9.

[15] Mohammad Al-Rabayah and Robert Maloney, Member, IEEE,"A New Scalable Hybrid Routing Protocol for VANETs", IEEE Transactions On Vehicular Technology, Vol. 61, No. 6, July 2012.

[16] M. Abolhasan, T. Wysocki and E. Dutkiewicz, "A review of routing protocols for mobile ad-hoc networks", Ad-Hoc Networks , Elsevier, pp. 1–22, 2004.

[17] B. Karp and H. Kung, "GPSR: Greedy Perimeter Stateless Routing for Wireless Networks" in: Proceedings of ACM MobiCom, 2000, pp. 243–254.

[18] Thangakumar Jeyaprakash, Nancy Vinoliya "Appraising Vehicular Ad-hoc Network Routing Protocols using NS2", International Journal of Information & Computation Technology, pp 491 – 498, 2014.

Rajeswari Mukesh has received her Ph.D. degree in Computer Science and Engineering from Jawaharlal Nehru University. Hyderabad. At present, she is a Professor and Head of Computer science and Engineering department at Hindustan University. She is guiding 8 PhD candidates. She has published more than 10 international journals and attended more than 15 international and National Conferences. Her area of specialization is Big Data, Biometrics, Ad-hoc Networks, and Cyber Security. She is a Member of IEEE & IET. She has won the "Women Engineer award" recently from IE

Thangakumar Jeyaprakash has received his B.E Degree in Electrical & Electronics Engineering from Dr. Sivanthi Aditanar College of Engineering, Tamilnadu in 2003, He obtained his M.Tech in Computer Science & Engineering, SRM University, Chennai. He is presently pursuing his Ph.D at Hindustan Institute of Technology & Science, Chennai, and Tamilnadu, India. He has Eight years of industrial, academic and research Experience. He is a member of IEEE, IET. His area of Interests is Mobile Ad-hoc Networks, Vehicular Ad-hoc Networks, Cryptography & Network Security, Data mining & software Engineering.